REMARKS

[0001] Claims 1 and 39-54 remain in the case and stand rejected. The Office Action objected to Claims 1, 39, and 50 for informalities. The Office Action objected to the Specification for lack of appropriate U.S. headings and a non-descriptive title. The Office Action rejected Claims 50-54 under 35 U.S.C. § 101 as being directed toward non-statutory subject matter. The Office Action rejected Claims 1, 39, 44, and 50 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,795,555 to Parisien et al. (hereinafter "Parisien"). The Office Action rejected Claims 40-43, 45-49, 51-54 under 35 U.S.C. § 103(a) as being unpatentable over Parisien in further view of European Patent Application No. 0999673 to Mamros et al. (hereinafter "Mamros").

AMENDMENTS TO THE CLAIMS

[0002] Applicants have amended Claims 1, 39, 44, and 50 to clarify embodiments of the invention. Applicants have amended Claims 42 and 43 for consistency with the amendments to Claim 44 and Claim 54 for consistency with the amendments to Claim 50. Applicants have cancelled Claim 53. The amendments are fully supported by the Specification, Claims, and Drawings. No new matter has been added.

AMENDMENTS TO THE SPECIFICATION

[0003] Applicants have amended the headings and title in the Specification. These amendments will be discussed in relation to the corresponding rejections and objections.

OBJECTION TO CLAIMS 1, 39, AND 50

[0004] The Office Action objected to Claims 1, 39, and 50 for informalities. Specifically, the Office Action stated that there is a lack of antecedent basis for the previously idle communications link. Applicants have amended Claim 1, 39, and 50 to clarify that the

-12-

"previously idle communications link" is the "idle communications link." Consequently, the Applicants respectfully request that these objections be withdrawn.

OBJECTION TO THE SPECIFICATION

[0005] The Office Action objected to the Specification for lack of appropriate U.S. headings and a non-descriptive title. Applicants have amended the title to recite "FACILITATING SECURE DATA COMMUNICATIONS THAT USE KEY-BASED ENCRYPTION." Furthermore, Applicants have amended the Specification to clarify the subject headings. Consequently, the Applicants respectfully request that the objection be withdrawn.

REJECTION OF CLAIMS 50-54 UNDER 35 U.S.C. §101

[0006] The Office Action rejected Claims 50-54 under 35 U.S.C. § 101 as being directed toward non-statutory subject matter. Specifically, the Office Action stated that the claim should recite "computer readable media" and describe the actions of the computer in present tense. Claim 50 has been amended to recite "A program product comprising a computer readable storage media embodying program instructions executed by a computer to facilitate . . ." (strikeout removed for clarity). In addition, as discussed during the telephone interview, Applicants have amended Claims 1 and 39 to recite a "computing node comprising a processor and a memory." Consequently, the Applicants respectfully request that the rejection under 35 U.S.C. 101 be withdrawn.

REJECTION OF CLAIMS 1, 39, 44, AND 50 UNDER 35 U.S.C. §102(e)

[0007] The Office Action rejected Claims 1, 39, 44, and 50 under 35 U.S.C. § 102(e) as being anticipated by Parisien. "Anticipation under 35 U.S.C. §102 requires the disclosure in a single piece of prior art of each and every limitation of a claimed invention. …Whether such art is anticipating is a question of fact." *Apple Computer, Inc. v. Articulate Systems, Inc.*, 234 F.3d 14, 20, 57 USPQ2d 1057, 1061 (Fed. Cir. 2000). It is well settled that under 35 U.S.C. §102 "an invention is anticipated if . . . all the claim limitations [are] shown in a single art prior art reference. Every element of the claimed invention must be literally present, arranged as in the

claim. The identical invention must be shown in as complete detail as is contained in the patent claim." *Richardson v. Suzuki Motor Co., Ltd.*, 9 U.S.P.Q.2d 1913, 1920 (Fed. Cir. 1989).

[0008] Parisien seems to describe an encryption scheme for use with terminal devices. Parisien, Abstract. Parisien appears to describe periodic key refreshes during system idle times. *Id.* at col 4, ll. 37-38.

[0009] Although the Office Action uses Mamros for a rejection under 35 U.S.C. 103, the amendment to Claim 39 introduces detecting that a heartbeat flowed across the communications link. The Office Action asserts that Mamros describes a heartbeat feature. Therefore, the discussion of the rejection under 35 U.S.C. 102 will include a discussion of Mamros. Therefore, Mamros appears to describe a system to determine the reachability of a remote computer over a telephone line. Mamros, Abstract. Mamros also appears to describe a protected keep alive message transmitted between computers that is not a rekey request. *Id.*

[0010] Applicants respectfully submit that amended Claim 39 recites features not taught or suggested in Parisien and Mamros. Claim 39 as amended states:

39. (Currently Amended) A method performed at a first ~~entity~~ computing node comprising a processor and a memory for facilitating secure data communications by using a secret key for encrypting data flowing between said first computing node and a second ~~entity~~ computing node comprising a processor and a memory over a communications link, the method comprising the ~~steps of~~:
  determining that the communications link ~~has been~~ is idle in response to detecting that a heartbeat flowed across the communications link;
  determining ~~whether~~ that data is available for flow over the ~~previously~~ idle communications link; and
  in response to a determination that data is available and a determination that the communications link is idle, initiating generation of a new secret key for use in encoding at least part of the available data before ~~it~~ the available data flows onto the communications link.

[0011] The amendments to Claim 1 find support in paragraph 68 and paragraph 75 of the Specification. Therefore, no new matter has been added.

[0012] Parisien and Mamros fail to teach "determining that the communications link is idle in response to detecting that a heartbeat flowed across the communications link" and "in response to a determination that data is available and a determination that the communications link is idle, initiating generation of a new secret key."

[0013] As discussed during the telephone interview, while Mamros seems to describe "keep alive" messages, Mamros fails to teach regenerating a secure key in response to a heartbeat having been transmitted due to an idle communications link. Furthermore, Parisien fails to teach heartbeats. Beneficially, renegotiating after a heartbeat has been issued provides extra security in case an attacker has managed to hack into the secret key.

[0014] Furthermore, neither reference teaches to regenerate the secret key when the communications link is idle *and when data is available*. Parisien describes refreshing keys during system idle times, Parisien, col. 5, ll. 29-34, and Mamros describes renegotiating when a certain amount of data has been transferred or when a certain amount of time has elapsed. Mamros, ¶ 32. However, neither reference makes a determination that data is available to send before renegotiating the secret key.

[0015] By renegotiating only when data is available to send, system overhead and resources are saved. For example, a communications link that is idle for a long period of time will continually renegotiate the secure key in a prior art system that performs that action on a timed basis.

[0016] Because Parisien and Mamros fail to teach the elements of Claim 39, Parisien and Mamros do not anticipate Claim 39. Consequently, Applicants respectfully request that the rejection of Claim 39 under 35 U.S.C. §102(e) be withdrawn.

[0017] Applicants respectfully assert that independent Claims 1, 44, and 50 are also not anticipated by Parisien and Mamros for at least the same reasons as independent Claim 39. Therefore, Applicants respectfully request that the rejection of Claims 1, 44, and 50 under 35 U.S.C. §102(e) be likewise withdrawn.

[0018] Furthermore, Claim 50 includes an additional limitation that "<u>only</u> in response to a determination that data is available to flow over the communications link <u>and a determination that the communications link is idle,</u> initiating generation of a new secret key" "<u>such that generation of a new secret key exclusively occurs when data is available for flow over the idle communications link.</u>" As stated above, neither Parisien nor Mamros makes a determination that data is available to send before renegotiating the secret key.

[0019] In addition, Claim 50, as amended, includes the following additional limitations:

> <u>sending a heartbeat message to the remote system only in response to determining that the link has been idle for at least a predetermined period of time and that there is no data available for flow over the communications link;</u>
> <u>monitoring the communications link for receipt of an acknowledgement from the remote system;</u>
> <u>receiving the acknowledgement from the remote system within a predetermined period of time;</u>
> determining <s>whether</s> <u>that</u> data is available for flow over the <s>previously</s> idle communications link; <s>and</s>
> <u>detecting that a heartbeat flowed across the communications link; and</u>
> <u>only</u> in response to a determination that data is available<u> for flow over the idle communications link and receiving the acknowledgement from the remote system within the predetermined period of time</u>, initiating generation of a new secret key for use in encoding at least part of the available data before <s>it</s> <u>the available data</u> flows onto the communications link<u>, such that generation of a new secret key exclusively occurs when data is available for flow over the idle communications link</u>.

The amendment to Claim 50 finds support in Claim 53, now cancelled. The amendment clarifies that a secret key is regenerated if an acknowledgement of the heartbeat is received. Therefore, if now acknowledgement is received, the resources and overhead necessary to generate a new key are not expended. The art of record includes no such teaching.

<u>REJECTION OF CLAIMS 12, 15, 29, AND 31 UNDER 35 U.S.C. §103(a)</u>

[0020] The Office Action rejected Claims 40-43, 45-49, 51-54 under 35 U.S.C. § 103(a) as being unpatentable over Parisien in further view of Mamros.

[0021] The Examiner bears the initial burden of establishing a *prima facie* case of obviousness. MPEP at § 2142. The prior art reference (or references when combined) must teach or suggest all the claim limitations. MPEP at § 2142. Furthermore, the factual inquiries for determining obviousness are summarized as follows:

1. Determine the scope and content of the prior art.
2. Determine the differences between the prior art and the claims at issue.
3. Resolve the level of ordinary skill in the pertinent art.
4. Consider objective evidence present in the application indicative of obviousness or nonobviousness.

Graham v. John Deere Co., 383 US 1, 148 USPQ 459 (1966).

[0022] Applicants assert that the Office Action fails to establish a *prima facie* case of obviousness, first because not all elements of the amended claims are taught or suggested in the art of record, and second, because the factual inquiry of Graham weighs in favor of nonobviousness.

SCOPE AND CONTENT OF THE ART

[0023] Parisien seems to describe an encryption scheme for use with terminal devices as described above. Parisien, Abstract. Furthermore, as stated above, Mamros appears to describe a system to determine the reachability of a remote computer over a telephone line. Mamros, Abstract.

DIFFERENCES BETWEEN THE PRIOR ART AND THE CLAIMS AT ISSUE

[0024] The Applicants respectfully assert that Parisien combined with Mamros fail to teach or disclose each element of the claimed invention.

[0025] As stated above in regards to Claims 1, 39, 44, and 50, Parisien and Mamros fail to teach "determining that the communications link is idle in response to detecting that a heartbeat flowed across the communications link" and "in response to a determination that data is available and a determination that the communications link is idle, initiating generation of a new secret key."

[0026]   Therefore, Applicants respectfully submit that Claims 12, 15, 29, and 31 are also different from Parisien and Mamros, depending on independent claims that are different from Parisien and Mamros. Therefore, Claims 12, 15, 29, and 31 are not obvious over Parisien and Mamros. Consequently, Applicants respectfully request that the rejection of Claims 12, 15, 29, and 31be withdrawn.

LEVEL OF ORDINARY SKILL IN THE ART

[0027] As stated in the MPEP, the "hypothetical 'person having ordinary skill in the art' to which the claimed subject matter pertains would, of necessity have the capability of understanding the scientific and engineering principles applicable to the pertinent art." Ex parte Hiyamizu, 10 USPQ2d 1393, 1394 (Bd. Pat. App. & Inter. 1988) (The Board disagreed with the examiner's definition of one of ordinary skill in the art (a doctorate level engineer or scientist working at least 40 hours per week in semiconductor research or development), finding that the hypothetical person is not definable by way of credentials, and that the evidence in the application did not support the conclusion that such a person would require a doctorate or equivalent knowledge in science or engineering.); MPEP 2141.03.

[0028] Therefore, Applicants respectfully submit that a person of skill in the art of the present invention is a person that has the capability of understanding the scientific and engineering principles applicable to data encryption and generating encryption keys.

OBJECTIVE EVIDENCE OF NON-OBVIOUSNESS

[0029] Applicants respectfully assert that the invention presented in the pending claims is sufficiently distinct from the prior art taught in Parisien and Mamros. The test for obviousness is what the combined teachings of the references would have suggested to one of ordinary skill in the art. *In re Keler*, 642 F.2d 413, 425, 208 USPQ 871, 881 (CCPA 1981). As previously noted, none of the prior references suggest renegotiating a secret key in response to detecting that a heartbeat has been issued. Furthermore, none of the references suggest renegotiating only when the communications link is idle and data is available to send.

-18-

[0030] The question is: would one in art when presented with Parisien and Mamros consider modifying one or the other to renegotiating only when the communications link is idle and data is available to send. Applicants submit that one in the art would not make such a leap.

[0031] Applicants submit that the features of their invention represent a nonobvious improvement over the art. Therefore, Applicants submit that the evidence weighs in favor of nonobviousness.

CONCLUSION

In view of the foregoing, Applicants submit that the application is in condition for immediate allowance. In the event any questions or issues remain that can be resolved with a supplemental phone call, the Examiner is respectfully requested to initiate a telephone conference with the undersigned.

Respectfully submitted,

Date: February 10, 2009
8 East Broadway, Suite 600
Salt Lake City, UT 84111
Telephone (801) 994-4646
Fax (801) 531-1929

/ David J. McKenzie /
David J. McKenzie
Reg. No. 46,919
Attorney for Applicants